

Legal Limits on Access to and Disclosure of Disaster Information

SUMMARY REPORT

Panel Members

Ralph C. Bledsoe, *Panel Chair*

Lawrence F. Ayers, Jr.

Louise K. Comfort

Gerald J. Mossinghoff

Janet L. Norwood

The views expressed in this document are those of the panel alone. They do not necessarily reflect the views of the Academy as an institution.

National Academy of Public Administration
1120 G. Street, N.W.
8th Floor
Washington, D.C. 20005

First published 1999

Printed in the United States of America

The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Permanence of Paper for Printed Library Materials, ANSI Z39.48.1984.

ISBN 1-5774-029-3

Legal Limits on Access to and Disclosure of Disaster Information



CONTENTS

FOREWORD by R. Scott Fosler	1
SUMMARY OF RESEARCH	3
FINDINGS AND RECOMMENDATIONS	13
PANEL AND STAFF BIOGRAPHIES	25

Officers of the Academy

Jonathan B. Howes, *Chair of the Board*
Feather O'Connor Houstoun, *Vice Chair*
R. Scott Fosler, *President*
Jane G. Pisano, *Secretary*
David S.C. Chu, *Treasurer*

Project Staff

J. William Gadsby, *Director, Management Studies*
Bruce D. McDowell, *Project Director*
Robert Lee Chartrand, *Senior Advisor*
Arnold Donahue, *Senior Research Associate*
Roger L. Sperry, *Senior Research Associate*
Lisa Warnecke, *Senior Research Associate*
Martha S. Ditmeyer, *Project Assistant*

Paul S. Hoff, *Garvey, Schubert & Barer*
Peter S. Vincent, *Garvey, Schubert & Barer*
Scott G. Warner, *Garvey, Schubert & Barer*

FOREWORD

In today's Information Age we seldom think about not having the data we need when we need it. Our greater concern seems to be coping with the overwhelming torrents of data that come at us from all directions. So, this study of limitations on data access and disclosure in the disaster management field may seem unusual.

But, it is both real and important. As one speaker said in helping to open the Academy's January 1999 conference on this topic, these data access and disclosure limits may well become the "pacing" element in implementing a National Disaster Information Network (NDIN). What he meant was that the speed with which an NDIN can be implemented is likely to depend on the speed with which the following can be accomplished:

- appropriate legal authorities can be agreed upon and established
- trust can be built among the multitudinous public and private partners, who need to be part of this network
- protections can be provided to avoid improper disclosures, and
- the quality of data can be improved to meet the needs of users while avoiding unnecessary liabilities

The Academy is pleased to have been invited to prepare this important report. We have drawn on the following recent Academy reports in the geographic information and emergency management fields to enrich this study:

- *Coping With Catastrophe: Building an Emergency Management System to Meet People's Needs in Natural and Manmade Disasters* (1993)
- *Geographic Information for the 21st Century: Building a Strategy for the Nation* (1998)
- *The Global Positioning System: Charting the Future* (1995)

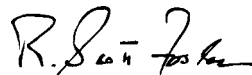
- *Reducing Seismic Risks in Existing Buildings: Options for Applying Federal Standards for Seismic Safety through Federal-Aid and Regulatory Programs* (1997)
- *The Role of the National Guard in Emergency Preparedness and Response* (1997)

These five reports bring together the two major elements of an NDIN—a strong understanding of disaster management and an equally strong understanding of geographic information issues. These studies explored and made recommendations about the roles of federal, state, and local governments, and the private sector, and the relationships among them.

The panel of experts assembled to prepare and guide this study shed a good deal of light on the very complex topic of limitations on data access and disclosure. It is essential that the issues addressed by the recommendations in this report be dealt with in a systematic and disciplined way from the very beginning of the enterprise. But, in many respects, this effort is just a beginning. As discussed in the report, much more research will be needed to fully understand and resolve issues in the four areas of concern.

The Academy believes that this study will serve well the purposes of those who become responsible for establishing an NDIN. Such a network has the potential to become one of the nation's most essential information tools for years to come, so it is of highest importance that it not be unnecessarily burdened by avoidable access and disclosure problems.

We want to thank the U.S. Geological Service and the members of the GDIN Transition Team, who were instrumental in getting this study included in the team's work program and were indispensable in helping us obtain excellent speakers and participants for the January 26, 1999 conference that was such an important part of this study. Special thanks also go to the busy people who served on the Panel and the staff who performed the research. The report has benefited greatly from all these contributions.



R. Scott Fosler
President

SUMMARY OF RESEARCH

BACKGROUND

In November 1997, a high-level Disaster Information Task Force consisting of federal officials from several key agencies, submitted to the Vice President a report entitled *Harnessing Information and Technology for Disaster Information*. That report recommended that the federal government begin to create an electronic disaster information network for the nation that could become a leading component of a worldwide Global Disaster Information Network (GDIN). The proposal projected the vision of a GDIN “as a robust, interactive knowledge base of disaster-related information accessible to disaster managers throughout the United States and to all whose lives and property might be affected by national disasters.”

The proposal projected the GDIN “as a robust, interactive knowledge base of disaster-related information...”

Under a cooperative agreement with the U.S. Geological Survey, signed September 22, 1998, the National Academy of Public Administration (Academy) undertook a preliminary analysis of certain legal limitations on access to and disclosure of disaster management data within the United States that will be important to consider in developing a national component of the GDIN. The legal limitations involve intellectual property, privacy, liability, and security concerns, but not issues concerning data that originate from classified national security sources (which are being studied separately).

DISASTER MANAGEMENT

The field of disaster management has evolved into an increasingly robust set of activities that embraces mitigation, preparedness, response, and recovery. Federal and other programs supporting this broadening range of activities now address manmade disasters as well as natural disasters, because the nation needs to be prepared equally for hurricanes, floods, or earthquakes, as well as for chemical spills, the inadvertent cutting of utility lines, and terrorist attacks. Other developments include the concept of disaster resistant communities, which is being promoted by the Federal Emergency Management Agency's Project Impact program. Increasingly, a continuous all-hazards approach to disaster management is emerging to help guide the large number of governmental and other organizations and programs that need to be involved.

...legal limitations involve intellectual property, privacy, liability, and security concerns...

Most disasters in the United States are local, and they are responded to by local governments, volunteer fire companies, non-profit and faith-based organizations, and others. A smaller number of disasters involve the states, and an even smaller number rise to the level of federally declared disasters. Nevertheless, management of these emergencies could benefit from having better information more readily available to support appropriate decisionmaking by responsible parties.

As the need for increasingly comprehensive, timely, and reliable disaster management information has increased in recent years, the technical ability to collect and manage data—including information about disasters, related phenomena, and the growing number of disaster-related programs—has improved strikingly, and these technical capabilities promise to continue improving rapidly. Unprecedented data accuracy, currency, and integration are becoming possible, and electronic communications capabilities now make it possible to share information almost instantaneously from one agency of government to another, from

one community organization to another, and from one nation to another.

THE PROPOSAL FOR A NATIONAL DISASTER INFORMATION NETWORK

The GDIN proposal recommends linking these newly emerging capabilities and organizations worldwide. As a first step, it focuses on creating a national disaster information network (NDIN) designed to serve the emergency management community within the United States. NDIN is proposed to be an electronically facilitated network that links many different databases, sources of information, disaster information centers, emergency management and crisis response centers, and information users. The proposed network would draw on and serve both the public and private sectors, and those involved will play a wide variety of roles. The network would operate throughout the four-phase disaster management process and be capable of addressing all hazards (both natural and manmade), including multiple-hazards (for example, when a flood causes fires, explosions, or toxic spills).

An NDIN is proposed to be a flexible and adaptable mechanism that brings together—but does not duplicate or displace the roles or responsibilities of—the various levels of government, the private sector, universities, and non-profit organizations for the common purpose of limiting losses from disasters. Some segments of the network would provide access that is fully open to all potential users including the public; other segments would provide access by a limited set of parties who have an established “need to know.” These multiple dimensions and purposes suggest that the network will be a complex socio-technical system that depends on the ability of personal and institutional behaviors to adjust to and take advantage of the new technological tools provided by an NDIN. Bringing all this together would require the use of public-private partnerships.

DATA ACCESS AND DISCLOSURE ISSUES FOR THIS STUDY

Clear access and data disclosure rules will be key to the smooth flow of critical information among the diverse partners involved in an NDIN.

The issues surrounding these rules may well become the “pacing” element in implementing an NDIN. The speed with which an NDIN can be implemented is likely to be determined by the speed with which:

- appropriate legal authorities can be agreed upon and established
- trust among partners can be built to enable easy and timely data sharing
- protections can be provided to avoid improper disclosures
- the quality of data can be improved to meet the needs of users and avoid unnecessary liabilities

This study examined these data access and disclosure issues and the legal limits to data access and disclosure. The study also endeavored to provide answers where possible. As expected, however, it was difficult to find clear or simple solutions to many of them. Thus, further studies will be needed on many issues.

...current... policies are conflicted between promoting open access to public information and... providing substantial protections against disclosing... sensitive information...

POLICY CONFLICTS

One of the most perplexing dimensions of data access and disclosure is the fact that current federal policies are conflicted between promoting open access to public information and “the right to know” about certain hazards that communities face, while simultaneously providing substantial protections against disclosing many types of private, proprietary, or other sensitive information. Many state and local policies mirror this dilemma, which is by no means unique to the disaster management field.

Legislators at all levels of government will have key roles in reconciling these diverse policies. However, finding the appropriate balance often will have to be done on a case-by-case basis during program administration.

FEDERAL PARTICIPATION

Federal government participation in developing public-private partnerships to find workable resolutions of data access and data disclosure issues is necessary if the full potential of the NDIN concept is to be realized. This reality should be addressed in the detailed design of an NDIN from the beginning. The design process should be a collaborative intergovernmental and public-private enterprise that takes into account data access and disclosure concerns of all partners.

POTENTIAL PROBLEMS

It is important to consider the potential problems of an NDIN from the beginning. For example, the more that an NDIN shapes the data in the network to help make it more useful to users, the more responsibility the network, itself, may have for liabilities resulting from the inappropriate use of these data. In addition, the more information that an NDIN compiles from diverse sources, the more likely the potential for breaches of privacy, confidentiality, and security. The network's designers should identify and address such problems as they proceed with their work.

RESEARCH ON LIMITS TO DATA ACCESS AND DISCLOSURE

This research has focused on the potential limits on access to and disclosure of disaster information that may arise from the four topics specified in the Academy's cooperative agreement with the U.S. Geological Survey. These topics are intellectual property, privacy, liability, and security. That research is summarized below.

INTELLECTUAL PROPERTY

Although a great deal of the information that needs to be available through an NDIN is publicly available, and it is the general policy of the

federal government to promote open access to most government information, there are three classes of information that may be restricted by intellectual property law and/or the actions of the owner of the information. They include copyrighted information, proprietary information, and trade secrets.

COPYRIGHTED INFORMATION

Access to copyrighted information is generally a matter of negotiating contracts or licensing agreements and paying fees or royalties for their use. There are many degrees of access to and ability to disclose copyrighted information, depending on the outcome of negotiations, law suits under the Freedom of Information Act, or other procedures.

The federal government may not copyright its own information, although it may hold copyrights transferred to it by others. In addition, the federal government, and persons representing it, may use any copyrighted or patented information without permission, subject only to paying reasonable royalties that are determined by court proceedings after the fact. Information generated for the government by another party is generally governed by Federal Acquisition Regulations and the contracts negotiated in accordance with them. These practices may vary among agencies, and sometimes allow the outside party to copyright such information to control its use by those other than the federal government.

In contrast, state and local governments, utility companies, and many private companies that may be expected to provide information to an NDIN, often copyright or otherwise restrict access to significant amounts of their information. Although many state and local governments have open access information policies similar to the federal policies, some governments are under pressure to recoup part of their database development and maintenance costs, and are doing so through charging fees for use of the information.

Generally speaking, databases are difficult to copyright under U.S. law. However, there are a few exceptions, and there is pressure from other nations to allow such copyrights. This issue is currently under consideration in Congress.

PROPRIETARY INFORMATION AND TRADE SECRETS

Access to proprietary information and trade secrets, as well as other sensitive information that is not copyrighted, may be harder for the federal government to gain and disclose. It is unlikely that trade secrets will be frequently sought for inclusion in an NDIN, but proprietary information, such as utilities' information on their infrastructure, may be more important to disaster managers. Although a few federal environmental laws have been enacted which override proprietary data claims by companies—based on the public's right to know about potential hazards—these are exceptional cases. Even under these laws, disclosure agreements have been negotiated to avoid revealing sensitive information. Similar techniques may be followed to obtain appropriate use of other proprietary information.

The extent to which intellectual property issues will limit access to and disclosure of information needed in an NDIN is likely to be determined incrementally as the system develops. Negotiations among data providers and users, continuing court cases, and evolving legislation may all play significant roles in the final determination.

PRIVACY

FEDERAL GOVERNMENT PRINCIPLES

The federal government's Privacy Act imposes a number of specific restrictions on the ability of a federal agency to make available personal information that it may have collected for another purpose. It is often the case that such disclosure requires the informed consent of each of the persons about whom information would be disclosed. The primary exception is when the information would be used for some other "routine" activity of the agency that is compatible with the original purpose for which the information was gathered.

These principles have been partially reflected in the Policy on Personal Information Privacy in Federal Geospatial Databases adopted by the Federal Geographic Data Committee (FGDC) in April 1998. In general, that policy statement says that "it is inappropriate to collect volumes of personal information simply because some of it may, in the future, prove

to be of some unanticipated value.” The policy also states that database users “should not use personal information in ways that are incompatible with the individual’s understanding of how it will be used, unless there is a compelling public interest for such use.”

The general provisions of the Privacy Act have been reinforced with a number of more specific provisions in laws such as the Computer Matching and Privacy Act of 1988, the Right to Financial Privacy Act, and the Driver’s Privacy Protection Act of 1994.

Database users “should not use personal information in ways that are incompatible with the individual’s understanding of how it will be used...”

STATE GOVERNMENT ACTIONS

Privacy protection by the states usually takes the form of exemptions to open records laws for certain information, such as information that is personal, confidential, related to law enforcement and investigations, part of preliminary internal agency activities, trade secrets, and proprietary or commercial. However, these provisions typically only exempt the sensitive information from mandatory disclosure under the applicable open records laws. They do not prohibit disclosure of the information, if the responsible government agency decides, in its discretion, to release the information in response to a request.

The laws in about 18 states, however, are stronger than this. They actually prohibit disclosure of sensitive information in the same manner as the federal privacy law, although with significant variations and exemptions. The use of private information for purposes other than those for which it was collected has seldom been allowed in these states. One example is comparison of state income tax records with child support records to assist in collecting child support. This technique is being used in a few states, but has been considered an invasion of privacy in others.

Interest in prohibiting the release of private information is growing as electronic information systems make it easier to collect, maintain, and disclose it. Such new technologies as Enhanced 911 emergency telephone systems and Intelligent Transportation Systems are providing new opportunities to gather improved location-specific information of value to emergency managers, but they also are raising new privacy concerns at the same time.

LIABILITY

POTENTIAL FOR LIABILITY

The liability of NDIN administrators for decisions made using information available through the network may be minimal if they do not provide information standards, or charge for access to the network, or warrant the information as being suitable for disaster management purposes. Passive NDIN administrators would be like an Internet provider; any liabilities created by using data obtained through it would be the responsibility of those who provided the information. However, to the extent that NDIN administrators take actions designed to ensure the quality and integrity of information available through the network and make it more useful to disaster managers and others, the NDIN administrators may take on some of the liability for the consequences of decisions based on the information.

LIMITING LIABILITY

The Federal Torts Claim Act would protect the federal government from liability for discretionary actions, but the exact extent of the government's liability will depend on what steps the government takes to limit its liability, and the facts of each case. It is possible in some states and circumstances that a court could conclude that the Federal Torts Claim act does not protect the government and that under state law the federal government is strictly liable for its role in an NDIN on the grounds that what it is providing through an NDIN is a product, not a service. State governments and private providers of information available through an NDIN may also be subject to "strict liability" for the information they contribute.

Those who provide information through an NDIN can try to limit their liability from the use of the information in the following ways:

- attaching disclaimer notices and metadata to the information
- producing the information using good professional practices, quality assurance procedures, and generally accepted data standards
- having their information certified as meeting good practice standards
- educating the information users to help them avoid misuse
- strengthening the protections of the Federal Torts Claim Act, and seeking other legislation to limit their liability for the use of information that is produced according to current standards of good practice

SECURITY

The information available through an NDIN should be secure from tampering and only available to those with a “need to know” should be protected against broader disclosure. The types of restricted-access information may include:

- detailed information about the nation’s critical infrastructures
- sensitive law enforcement, utility, and casualty information
- privileged, proprietary, and sensitive information
- classified national security information
- private information about individuals

The federal Computer Fraud and Abuse Act of 1986, as amended, makes it a crime to gain unauthorized access to electronic information and to alter it. The Electronic Communications Privacy Act of 1986 prohibits unauthorized interception of electronic communications while in transit. Most state and local laws also appear to have addressed these and similar issues to various degrees. A more comprehensive study of the adequacy of existing information security laws may be needed.

Based on this study’s research, the panel offers the following findings and recommendations.

FINDINGS AND RECOMMENDATIONS

FINDINGS

1. MANY DATA AFFECTED BY LIMITS

Many types of information proposed to be available through an NDIN will be affected by access and/or disclosure limitations that grow out of concerns about protecting intellectual property, privacy, and security, and holding parties liable for damages to which they may have contributed. The legal principles growing out of these concerns may place limits or disincentives on the ability to (1) gain access to significant amounts of the information needed, (2) disclose some of the information openly to others through the network, and (3) withhold some information even when required by some provisions of law. Some examples of data access and disclosure limitations follow.

- Increasingly, commercial sources are being relied on by governments for information derived from and including satellite imagery, photogrammetry, land surveys, navigation charts, base maps, enhanced weather information, and integrated disaster information in easy-to-use GIS packages, as well as a host of other geographically referenced information that is essential to mapping and understanding the characteristics of communities and to managing disasters. Such information is likely to be under copyright and/or license agreements that may limit its use and disclosure to broad audiences.
- Utility information often is difficult to obtain and use for public purposes because it is technically unavailable, proprietary, confidential, or withheld to guard against sabotage or terrorist attack.

- Helpful information from classified national security sources may be difficult and time-consuming to access, and its disclosure is restricted.
- Historical information about repetitive losses (from floods for example) may be difficult to obtain for mitigation planning because it is considered proprietary by insurance companies and/or an invasion of privacy by the affected parties.
- The presence of hazardous materials—knowledge that disaster managers need to have in preparing for and responding to emergencies—may be deemed proprietary or confidential.
- Information about the occupancy of buildings—including numbers of people and how many may have disabilities or other special medical conditions—which may be critical for preparedness planning, may be considered proprietary or private.
- Inaccurate maps, charts and decisions—that could allow buildings to be inappropriately located in hazardous places, or could delay emergency responses—may give rise to liability suits if loss of life, serious medical consequences, or property damages can be traced to them.
- Improper access to private, proprietary, or confidential information through an NDIN could bring lawsuits.

2. PRECISE LIMITS NOT IDENTIFIED

Limitations on access to and disclosure of the specific data elements that may be available through the proposed NDIN, and the means of accommodating them, cannot be precisely identified until more is known about the features and intended uses of the network. These limitations will become more apparent as specific data elements become available through the network and begin to be used for specific purposes by specific parties under specific circumstances.

3. LESSONS FROM OTHER FIELDS

Lessons for accommodating data access and disclosure limitations associated with an NDIN may be available from other fields, such as

the field of geographic information systems (GIS). The need to deal with the issues of protecting intellectual property rights, privacy, and confidentiality, and guarding against liabilities arising from the use and misuse of data is not unique to an NDIN. Neither is the idea of developing distributed electronic information networks. There is a large body of experience on these subjects that has evolved in other fields, such as GIS, and could be drawn on to help guide the development of an NDIN. Although lessons from related fields do not always provide clear or simple guidance, and such lessons are still evolving as new issues are raised by the rapid development of the electronic information age, they provide an essential starting point. The potential of these lessons for helping to avoid data access and disclosure problems may be significant.

This study identified 18 federal laws and regulations that must be examined and considered concurrently in the data access and disclosure field.

4. COMPLEXITIES AND INCONSISTENCIES

The current array of federal, state, and local laws, regulations, and practices that limit data access and disclosure is highly complex, and the many separate provisions are not always consistent and often conflict with each other. Some examples of these complexities and inconsistencies follow.

- Tensions exist between federal freedom of information, privacy, and confidentiality laws. This study identified 18 federal laws and regulations that must be examined and considered concurrently in the data access and disclosure field.
- State laws on freedom of information, privacy protections, and protection for trade secrets vary widely across the country. For example, 21 states have privacy laws that are separate from their public records laws, 30 states have separate trade secrets laws, and all states have special laws that grant or withhold access to specific types of information.

- State and local practices also vary widely with respect to conditions and prices charged for access to GIS databases. At least eight states limit access to their GIS databases and charge higher fees for them than they charge for access to other public records. In addition, a recent survey of large cities and counties found that 80 percent restrict access to their GIS databases in some way.
- Liability laws apply largely on a case-by-case basis. When data obtained through an NDIN are judged to be products, rather than services, the “strict liability” doctrine applies. In such cases, the data are viewed as products suitable for the purpose for which they are offered, and if a user sustains loss as a result of relying on them, the NDIN could be held liable.

Designers of an NDIN must navigate these uncertainties. It will be difficult to provide definitive advice to guide the design and implementation of the network as long as these matters remain unsettled.

5. INTERNATIONAL IMPLICATIONS

Unresolved international intellectual property proposals pertaining to databases, as well as new privacy protection conventions, may have significant impact on U.S. practices.

Designers of an NDIN must also resolve these complexities and uncertainties, since it will be difficult to guide the design and implementation of the network as long as the underlying laws, cases, treaties, and practices remain so diverse and unsettled.

RECOMMENDATIONS

RECOMMENDATION 1. GENERAL PRINCIPLES

Incorporate the following general principles for data access and data disclosure into the design of an NDIN from the beginning:

- **Open Disclosure:** As much disaster management information as possible should be made available through the open access portion of an NDIN.

- **Rules and Disclaimers:** Develop and communicate clear and understandable rules and disclaimers about access and disclosure.
- **Restricted Access:** Any of the following information that may be available through an NDIN should be treated with great care and specific legal and technical safeguards should be devised to ensure that it is available only to those who need it:
 - sensitive information about specific individuals, companies, or organizations, and copyrighted data
 - classified national security information or information derived from classified sources that continues to need protection
 - information about critical infrastructures that might compromise the security of those systems or facilities

It should be noted that, under current law, such firewalls may not always be sufficient, by themselves, to protect information from discovery under FOIA, or to necessarily avoid a violation of the Privacy Act. For this reason, the President's Commission on Critical Infrastructure Protection has recommended an amendment to FOIA to exempt certain critical infrastructure information from public disclosure. Further study of this issue should be undertaken.

...firewalls may not always be sufficient... to protect information from discovery under FOIA...

- **Review of Restricted Data:** To the extent that an NDIN must contain and use sensitive or classified information (as defined above) to perform its functions adequately, such data should be reviewed regularly to determine the extent to which its disclosure still needs to be restricted.
- **Aggregated Data:** Data that is aggregated into statistical summaries sufficient to meet the purposes of disaster managers, but general enough to avoid disclosing information that is sensitive,

classified, or that might breach the security of the nation's critical infrastructures, should be disclosed to the public.

- **Data-Sharing Agreements:** Agreements should be negotiated with those supplying data to the network to establish precise conditions for data access, use, and disclosure. It is especially important to have these agreements, as well as implementation resources and mechanisms, in place ahead of time to ensure that the information needed immediately in times of emergency will be readily available.
- **Data Integrity and Security:** The information shared through the network should be sufficiently reliable to be used in disasters and secure enough to deter tampering. Such tampering could have significant implications for liability and other data quality concerns.

RECOMMENDATION 2. DESIGN IMPLICATIONS FOR DATA ACCESS AND DISCLOSURE

Conduct detailed studies and conferences to help define more precisely the specific data elements that need to be acquired and disclosed to identified parties for identified disaster management purposes. These activities should clarify the nature of an evolving NDIN and the disaster management decisionmaking processes it is designed to support.

The design implications... are very significant for data access and data disclosure issues...

The current status of the NDIN as an “empty vessel” into which disaster-related information can be poured may not provide an adequate basis for supporting improved disaster management. Each of the four phases of disaster management—mitigation, preparedness, response, and recovery—requires somewhat different sets of information to support distinctive decision processes involving different sets of decision

makers and constituencies. Some of these processes are more real-time than others, some are more oriented to the general public than others, some need more precise data than others, and some have greater requirements for sensitive, classified, or other limited access data than others. To help achieve disaster management goals—reduced losses of life, property, and economic and social functions of society—the users of an NDIN increasingly may expect the network to deliver disaster management information in integrated user friendly decision-support packages.

The design implications for the NDIN of these diverse disaster-decision processes are very significant for data access and data disclosure issues, as well as for other issues. The network's design should identify which types of data will be available only with secure restricted-access, which will have open access, and how the system will provide tamper-proofing arrangements for all data. Specific studies should address the following topics:

- the adequacy of legal and technical means for protecting restricted information
- a detailed examination of unauthorized-tampering laws
- a 50-state search and analysis of state laws addressing information security issues and restrictions on disclosing personal and confidential information
- a synthesis of the GDIN Transition Team's first round of studies which provide significant new information about data needs, decisionmaking needs, interoperability of electronic information systems, and institutional issues
- lessons from existing information clearinghouses and networks (for disaster management and other purposes) in the federal government, in state and local governments, and in other countries, that could help to further define data access and disclosure arrangements, and their benefits, pitfalls, and critical success factors
- a more detailed assessment of exposures to liability related to the transmission and use of specific types of disaster information

RECOMMENDATION 3. BEST PRACTICE STUDIES AND MODELS

Develop a series of “best practice” models to assist legislators, designers, and users of the NDIN to simplify and mitigate data access and data disclosure issues. These models should be based on detailed studies, and should be designed to meet the special needs of each phase of disaster management.

Research is needed to identify good practices more precisely than was possible in this study; conferences of affected parties are needed to identify and reach agreement on acceptable features of the models to be recommended; and appropriate actions should be taken to promote widespread acceptance and use of the identified practices and models. This research should analyze current conditions, inventory the relevant laws and practices of the 50 states, analyze the pros and cons of alternative approaches, and highlight the most promising options. Some of the models that should be considered are:

- **State Legislation.** Suggested state legislation—and related policies and regulations—should be developed to amend differing state freedom of information, privacy, trade secrets, GIS, copyright, utility regulation, and electronic information security laws in ways that would facilitate the purposes of an NDIN.
- **Federal Laws and Policies.** Amendments should be drafted to clarify and reconcile differing federal policies, laws, and regulations, including OMB Circulars and Executive Orders that relate to intellectual property, privacy, freedom of information, liability, and civilian use of information derived from classified sources.
- **U.S. Positions on International Issues.** Well-defined U.S. positions on the use of electronic databases and privacy protections should be developed to provide credible alternatives to the positions of other nations when negotiating international treaties on these issues.
- **Data-Sharing Agreements.** Model agreements—and models of supporting institutions, processes and practices—should be developed to facilitate fair, equitable, and effective data sharing,

licensing, and pricing relationships among public and private data producers participating in an NDIN.

- **Data Quality Assurance.** Models should be developed to facilitate adoption and maintenance of data quality assurance and certification programs to improve the accuracy, reliability, timeliness, relevance, completeness, and credibility of the information available through an NDIN, and to help reduce the potential for liability of the network and its data suppliers and users.
- **Liability Limits.** To help limit liability, models should be developed concerning:
 - disclaimers
 - metadata standards to establish the accuracy, timeliness, and suitability for intended purposes of the data available through an NDIN
 - the use of outside companies to certify the quality of disaster management data
 - legislation limiting liabilities resulting from the use of properly prepared and documented data
- **Partnerships with the Private Sector.** Models should be developed to facilitate the use of public data trusts, public-private partnerships, and other institutional mechanisms that could help to facilitate access to and disclosure of data through an NDIN.
- **Regional Demonstrations.** Selected demonstration projects should be conducted to show how disaster information networks would function at the metropolitan or regional level.

Research is needed to identify good practices...

RECOMMENDATION 4. AWARENESS AND CAPACITY

Provide information about potentially applicable data access and disclosure limitations to an NDIN's designers, data suppliers, and users.

Even for those who are directly involved, dealing with these issues is difficult. For those not directly involved, such issues are almost invisible. Yet, these key issues may cause significant problems even for casual users. Thus, there is a considerable need for everyone involved in an NDIN to be aware of these issues and prepared to deal with them.

There is... considerable need for everyone involved... to be aware of these issues...

This need might be satisfied through efforts by all the partners to supply printed materials, conferences, and training opportunities geared to the needs of different participants in the network. For the most intensively involved designers and strategists, detailed information should be provided to give them the capacity to effectively cope with the complexity of the issues. This information should be updated regularly as additional good practices are identified, and as current issues get resolved.

RECOMMENDATION 5. THE FEDERAL GOVERNMENT'S ROLE

Make data access and disclosure principles an integral part of the federal government's effort to continue developing the NDIN concept and disaster information resources. These federal efforts should be pursued in collaboration with other public, private, university, and non-profit parties, and they should include sponsoring a metadata clearinghouse for disaster information.

A continuing federal role is necessary to facilitate the nationwide approach needed if an NDIN is to work as intended within the United States and link appropriately to the rest of the world. The federal government should continue its important role in the NDIN by functioning as a:

- catalyst for collaboration and partnership
- contributor of many of the essential elements in the network
- sponsor of demonstration projects, information and training resources, and efforts to produce standards and definitions that

can help to reconcile disparate data access and disclosure policies and improve the consistency and quality of disaster management data

- sponsor of a metadata clearinghouse to document the quality of disaster information

Because an NDIN will likely transmit information resources from a wide variety of sources—including federal, state, and local governments, utility and other companies, universities, and non-profit organizations, it should be built by a collaborative national program, based on existing databases that can be interrelated and used now (with careful attention to their quality and metadata), and improved incrementally over time to form an evolving network of increasingly useful federated databases. Federal mandates should be avoided, but federal leadership should be used to help catalyze state, local, and non-governmental action.

The federal government should... sponsor a metadata clearinghouse to document the quality of disaster information.

Much of the information needed by disaster managers is geographic information that is already becoming available through the National Spatial Data Infrastructure (NSDI) sponsored by the Federal Geographic Data Committee (FGDC). That information is consistent with evolving metadata approaches and standards, and with FGDC's recently adopted Policy on Personal Information Privacy. Thus, building on the previously established elements of the NSDI will avoid duplication of effort and facilitate development of an NDIN that will already incorporate some sound data access and disclosure policies. The geographic data coordination programs of the FGDC, and its state and local counterparts, provide appropriate models to follow in building an intergovernmental and public-private NDIN.

Other new tools that could be used to help an NDIN of federated databases become increasingly useful for disaster managers include:

- the improving commercial technologies for merging and integrating diverse geographic data files
- the growing interoperability of geographic data software
- the increasing tendency to capture geographic data from public and private transactions as they occur, which provides greater timeliness of data than in the past

PANEL AND STAFF LIST

PANEL

Ralph C. Bledsoe, *Panel Chair*—Former Assistant Archivist for Policy and IRM and for Management and Administration, National Archives and Records Administration; Director, Ronald Reagan Library; Director, Washington Public Affairs Center, University of Southern California; Special Assistant to the President of the United States, Domestic Policy Council and Cabinet Council on Management and Administration; Associate Director, Office of Planning and Evaluation, Federal Emergency Management Agency; Professor and Senior Faculty Member, Federal Executive Institute.

Lawrence F. Ayers, Jr.*—Executive Vice President, Intergraph Corporation; former Civilian Director, Defense Mapping Agency; key participant in charter to consolidate the Army, Navy and Air Force assets into the Defense Mapping Agency. Panel Member for the Academy study of geographic information (1998).

Louise K. Comfort*—Associate Professor of Public and International Affairs, University of Pittsburgh; principal investigator/project coordinator on a variety of research initiatives relating to disaster management, risk management, and hazardous materials; Research Associate, Institute of Governmental Studies, University of California, Berkeley. Panel Member for the Academy study of seismic safety (1997).

Gerald J. Mossinghoff—Professor, George Washington University School of Law; former President Pharmaceutical Manufacturers Association; Assistant Secretary of Commerce and Commissioner of Patents and Trademarks; Chairman, General Assembly of the United Nations World Intellectual Property Organization; Deputy General Counsel, National Aeronautics and Space Administration.

Janet L. Norwood—Senior Fellow, The Urban Institute; former U.S. Commissioner of Labor Statistics, U.S. Department of Labor; Research Associate, William L. Clayton Center, Fletcher School of Law and Diplomacy, Tufts University.

* Not an Academy Fellow

STAFF

J. William Gadsby, *Director of Management Studies*—National Academy of Public Administration; project director on several recent Academy studies, Former Senior Executive Service; Director, Government Business Operations Issues, Federal Management Issues and Intergovernmental Issues, General Accounting Office.

Bruce D. McDowell, *Project Director*—Former Director of Government Policy Research and Assistant to the Executive Director, U.S. Advisory Commission on Intergovernmental Relations; Director of Governmental Studies, National Council on Public Works Improvement. Director of Program Coordination, Metropolitan Washington Council of Governments.

Robert Lee Chartrand, *Senior Advisor*—Advisor to U. S. Congress on Y2K and emergency management issues. Former Senior Specialist and Senior Fellow, Information Policy and Technology, Congressional Research Service. AAAS fellow. Recipient of the 1985 ASIS Award of Merit and the Library of Congress Award for Superior Service in 1988.

Arnold E. Donahue, *Senior Research Associate*—President, Pactrade, Inc.; Former Senior Executive Service, Chief, Command, Control, Communications and Intelligence, Office of Management and Budget; Intelligence officer and economist, Central Intelligence Agency.

Roger L. Sperry, *Senior Research Associate*—Former Director of Management Studies, National Academy of Public Administration; former Professional Staff Member, U.S. Senate Committee on Governmental Affairs; Senior Group Director and Special Assistant to the Comptroller General, the U.S. General Accounting Office.

Lisa Warnecke, *Senior Research Associate*—Author of the *State Geographic Information Activities Compendium*; co-founder of the National States Geographic Information Council; principal investigator, *National Study of Information Resources Management in State Governments*; Town Manager in Colorado.

Martha S. Ditmeyer, *Project Assistant*—Consultant, National Academy of Public Administration. Former staff member at the Massachusetts Institute of Technology and the Communications Satellite Corporation.

GARVEY, SCHUBERT & BARER

Paul S. Hoff, *Partner*—Former Deputy General Counsel of the Senate Governmental Affairs Committee, author of American Enterprise Institute study, “Inventions in the Marketplace.”

Scott G. Warner, *Partner*—Specialist in high technology companies and other emerging growth companies, with an emphasis on computer law, electronic commerce, international regulation of the Internet, protection of intellectual property rights and franchise and trade regulation.

Peter S. Vincent, *Associate*—Former Editor-in-Chief of the *Virginia Journal of International Law*. Specializes in complex state and federal litigation.